GEORGIA SOUTHERN UNIVERSITY

BRING YOUR OWN DEVICE (BYOD) POLICY

Area:	Information Technology	Number:	
Applies to:	University Community	Issued:	June 2, 2014
Sources:		Revised:	May 18, 2020
		Reviewed:	
Policy Owner:	Chief Information Officer	Page(s):	2

I. Purpose

This policy is established to secure the use of personally-owned devices while preventing Georgia Southern data from being deliberately or inadvertently stored insecurely and potentially being accessed by unauthorized resources. This policy applies to the University Community. Adherence to this policy helps safeguard the confidentiality, integrity and availability of the University's information assets, and protects the interest of the University, its customers, personnel and business partners.

II. Policy Statement

Mobile computing is an increasing part of everyday life, as devices become smaller and more powerful, the number and complexity of tasks that can be achieved away from the office continues to expand. As the capabilities of these resources increase, so too, do the risks. The following security controls have been created to protect University resources, including data, when using a personal mobile device(s).

As defined in the USG IT Handbook Section 8, employees or contractors acting on behalf of Georgia Southern who are using personally-owned devices to access Georgia Southern data will ensure such devices employ the appropriate device protections such as, but not limited to, passcode, facial recognition, card swipe, etc.

Users who are authorized to access Georgia Southern resources and data are authorized to use BYOD devices as long as they comply with Georgia Southern's Acceptable Use Policy (AUP) and BYOD policy.

The use of BYOD devices to access sensitive and confidential University data implies user compliance with these required practices.

III. Definitions

Personal / Mobile Devices: Any personal electronic device that connects to University resources, including but not limited to: Laptops, Notebooks, Tablet devices, Smartphones, and Smart Watches.

Computing Resources: All University information processing resources including all University owned, licensed, or managed computing services, hardware, software, and use of the University

network via physical or wireless connection regardless of the ownership of the computer or device connected to the network.

University Data: All data owned or licensed by the University.

University Community: Includes faculty, administrators, staff, student workers, graduate/technical assistants, alumni, interns, guests or agents of the administration, external individuals and organizations accessing University network services, and other authorized users.

IV. Exclusions

There are no exclusions or exceptions to this policy.

V. Procedures

Privacy/company access

No person using his or her personal device should expect any privacy except that which is governed by law. Georgia Southern University has the right to monitor the use of and preserve any communications that use Georgia Southern's resources in any way, including but not limited to: data, voice mail, telephone logs, Internet use and network traffic, for the purposes of compliance and determine appropriate use.

Lost, stolen, hacked or damaged equipment

Users are expected to protect personal devices used for work-related purposes from loss, damage and theft. Strong passwords are required to be set on all devices. In keeping with best practices for BYOD devices, it is recommended that all devices utilize encryption and maintain a functioning and up to date anti-virus solution. Devices should be patched to appropriate and supported OS versions.

Georgia Southern will not be responsible for loss or damage of personal applications or data resulting from the use of company applications. Employees must immediately notify IT Services in the event their personal device is lost, stolen or damaged.

Compliance

The University reserves the right to audit any personal electronic device using University resources to ensure compliance with this policy. Instances of non-compliance must be presented to and reviewed and approved by the CIO, the Chief Information Security Officer or equivalent officer(s). All breaches of information security, actual or suspected, must be reported to, and investigated by the Chief Information Security Officer.

Any individual(s) that violate security policies, standards, or security procedures are subject to disciplinary action up to and including loss of computer access and appropriate disciplinary actions as determined by the University.